ABSTRACT

One aspect of the invention provides a novel scheme to protect content stored in a non-volatile storage device from unauthorized modifications and/or access. The non-volatile storage device is configured as one or more regions, one or more of the regions implementing one or more content protection schemes. The current version of content stored in a region is compared to a previously stored valid version of the content to determine if the current version has been modified without authorization. A region may be protected by use of an integrity metric (e.g. checksum, bit mask, and/or cyclic redundancy check value).

The invention may be implemented during the start-up sequence of a computer system to protect the system's Basic Input Output System (BIOS) from unauthorized modifications.